Using SOC1 To Build An Effective Control Environment

An SVA Perspective

SVA | Certified Public Accountants

Tax, Audit and Business Strategy

Using SOC 1 To Build An Effective Control Environment
An SVA Perspective

Introduction

Effective risk management depends on an enterprise's ability to establish and maintain a strong control environment. Such an environment has become paramount in the financial services industry given prevailing business conditions, increasing complexity, and evolving regulations. But how can management establish and maintain a strong control environment? When it has done so, how can management demonstrate that fact to customers, investors, and other stakeholders?

One good answer to those questions is SOC 1 (formerly referred to as SAS 70).

SOC 1 refers to the Reporting on Controls at a Service Organizations, issued by the American Institute of Certified Public Accountants (AICPA). A SOC 1 report is an examination of an organization's controls as they relate to transactions that affect or can affect the financial statements of other organizations. Organizations that have not engaged in a SOC 1 examination can find it quite useful to do so for several reasons. Primarily, the examination can help an organization to build out an effective control environment by providing a mechanism for assessing risks, implementing controls to mitigate risks, evaluating the design of controls, and periodically testing the effectiveness of the controls.

This paper charts a path to excellence in risk management. Taking a less "philosophical" approach than many papers, this document explains how SOC 1 can help management create a strong control environment which is the cornerstone of sound risk management in any enterprise. Note that SOC 1 is one tool for management to use to strengthen the control environment and to support and evidence good governance and sound risk management, rather than constituting a risk management framework. For instance, SOC 1 does not cover all the factors that a risk management framework would, nor does it enforce leading practices. Instead it evaluates whether controls are sufficient to meet the specific control objectives in scope of the report.

That said, establishing a strong control environment demands an examination of the organization's business objectives and key risks. Then there must be a determination that the appropriate level of controls has been designed and implemented to manage these risks on an ongoing basis. In addition, there should be a means of documenting and demonstrating the control environment to relevant parties. SOC 1 enables an enterprise to accomplish these tasks by providing guidance for the examination and documentation of controls.

Incidentally, SOC 1 defines a "service organization" (to which SOC 1 applies) as any organization that processes transactions that can affect the financial statements of customers. This means organizations that execute transactions for others and maintain the related accountability or record transactions and process the related data or both. This includes enterprises in healthcare billing and most types of claims processing and data centers as well as trust departments, investment advisers, asset managers, and administrators of retirement, employee benefit, and similar plans. SOC 1 can potentially increase the performance and professionalism of any such company not currently employing the standard. Despite this, little has been said about the value of SOC 1 in this regard. Indeed SVA has found that SOC 1 is often misunderstood although it is becoming accepted as the standard in ascertaining the quality of control environments in service organizations. Thus, clearing up such confusion is yet another aim of this paper as is pointing out the potential benefits of SOC 1.

An Increasingly Useful Tool

SOC 1 is a standard from the AlCPA for examinations of service organizations' controls that affect customers' financial statements. Given the prevailing risk and regulatory environment, it is becoming clear that organizations that do not have a SOC 1 available may be at a competitive disadvantage in developing new business.

In general, self-inspection and lack of transparency have created substantial risks and problems for service organizations of all sizes since the recession of 2008-2009. Given this, it is worth considering that, when properly executed, SOC 1 can assist management in designing and implementing controls that fit its business processes while meeting the needs of relevant stakeholders for information regarding the control environment.

What is SOC 1?

SOC 1 is neither a certificate nor an award, nor does it impose a set of standards on a company. It is neither a one-day exercise nor a checklist audit. It is not required for all service organizations (although Section 404 of the Sarbanes-Oxley Act of 2002 increased the importance of SOC 1).

Issued in 1992, SAS 70 (the former version of SOC 1) focuses on the effects that organizations that process or record data or transactions for other organizations can have on the financial statements of their customers. Back then the central question was: What standards should apply to independent auditors when they prepare statements that other auditors will rely on? SAS 70 answered that question.

Since then the importance of SAS 70 and now SOC 1 has increased with the expansion of the financial marketplace and enterprises' increasing use of third-party service providers. When an enterprise uses a service organization to process or record data or transactions, it exposes its financial statements- and the underlying transactions and accounts to policies and procedures it does not completely control. Thus, to some extent, the enterprise relies on the control environment of the service organization. Similarly, customers' auditors rely on service organizations' records. So it is in a service organization's or asset manager's interest to maintain a strong control environment and to document the presence of that environment.

A SOC 1 supplies that documentation. If you have only heard of SAS 70 or SOC 1, it may have been from a customer or prospective investor requesting a SOC 1 report. That report describes your organization's processes and controls as they affect customers' data and transactions. A SOC 1 examination is the means by which the report is produced. It is also a vehicle for strengthening your control environment and risk management infrastructure.

Types of SOC 1 Reports

There are two types of SAS examinations and each results in a different type of report - a Type 1 or a Type 2 report.

A Type 1 report provides two opinions of the independent auditors regarding the service organization's controls on a specific date. First, the report presents the auditor's opinion of whether the organization's description of its controls presents a fair and accurate picture of the controls in place on that date. Second, it includes the auditor's opinion of whether the controls on that date were designed to achieve the organization's stated control objectives.

A Type 2 report presents the two opinions presented in a Type 1 report, as well as the auditor's opinion of whether the controls tested were operating so as to provide reasonable assurance that the control objectives were achieved during a specific period, usually 12 months.

Type 1 examinations provide limited value compared with Type 2 examinations. Type 1 is usually undertaken in the first year after adopting SOC 1. When an investor or auditor from another organization requests a SOC 1, they are usually referring to a Type 2 report. Exhibit 1 summarizes the key differences between the two reports.

Exhibit 1: Key differences between Type 1 and Type 2 SOC 1 reports

Report	Applicable timeframe	Opinion of controls
Type 1	As of a specific date	Covers design & implementation
Type 2	Covers a period of time (usually 6 to 12 months)	Covers design, implementation, & effectiveness

What SOC 1 Does

SOC 1 is widely recognized as a leading practice and SVA views the SOC 1 process as a path to increasing efficiency and effectiveness of controls and risk management. Moreover, it makes sense from business and marketing standpoints. Many investors and customers seek evidence of a strong control environment as part of their request for proposal (RFP), request for information (RFI), and due diligence processes. They are also driven to request a SOC 1 report by several other concerns and benefits.

A SOC 1 examination usually occurs in two phases - a readiness assessment and the examination itself. In a sizable organization, a readiness assessment can require elapsed time of 6 to 12 weeks and a Type 2 examination can require 10 to 14 weeks. All too often an organization unfamiliar with SOC 1 will suddenly discover that a prospective customer requires a Type 2 report as part of its due diligence or contracting process. If the report has not been prepared, that business opportunity may be lost.

Thus it is wise from a business development standpoint, as well as from a risk management standpoint to perform a SOC 1 readiness effort before a report is needed. To this end, SVA is seeing organizations that have not yet committed to moving forward with a formalized SOC 1 go through a diagnostic process, like the readiness assessment, to position themselves to execute a SOC 1 when a specific need arises. Moreover, an enterprise can realize a number of other operational and risk management benefits from a readiness assessment.

Why Investors Request a SOC 1

Not all parties can obtain access to a service organization’s SOC 1 report, given that its distribution is typically subject to the terms of the engagement letter between the service organization and the independent auditor. However, investors are increasingly requesting a SOC 1 report because it:

- Is a necessary item in their due diligence or vendor contracting process
- Provides a picture of a fund’s commitment to risk management
- Attests to the rigor of their control environment when they are scrutinized by others
- Serves as an element in their leadership’s oversight responsibilities
- Makes it easier for their auditors to construct their financial statements
- Saves them the expense of visits and documentation requests

A SOC 1 Readiness Assessment

In a readiness assessment, the enterprise:

- Determines the scope of the engagement, which can cover the entire service organization, or one or more businesses or products, and areas considered as optional in a future SOC 1 report
- Conducts a broad risk assessment within the areas defined by the scope
- Gathers and leverages existing control documentation (such as operational policies, procedures, and checklists)
- Interviews heads of the areas and control owners to identify relevant control activities (such as reconciliations and approvals)
- Creates a Risk and Control Matrix to outline the relevant control objectives and associated control activities
- Identifies control gaps and necessary enhancements to meet the required control objectives and identifies suggestions for non-control related improvements in people, processes, and technology
- Provides recommendations to management to consider relating to control objectives to be included in a future report addressing the identified risks (such as segregation of duties)
- Identifies documentation which control owners may have to produce to evidence the performance of control activities

A SOC 1 Examination

In a SOC 1 examination, independent auditors:

- Meet with management to develop an engagement plan, assign roles and responsibilities, gather documentation, and agree on the approach and timing of the examination
- Inspect the controls to ascertain whether they are in place and effectively designed
- Test the effectiveness of the controls by interviewing personnel, observing specific controls, inspecting documents indicating performance, and re-performing controls
- Prepare and issue a Type 1 or Type 2 Report depending on whether the effectiveness of controls was tested

SOC 1 Benefits

Long a leading practice, SOC 1 is becoming the standard for service providers who want to achieve excellence in processes that serve their customers. SOC 1 can enable such enterprises to:

- Meet investors' and customers' requirements: As part of their due diligence and contract procedures, many investors and customers routinely request a SOC 1 report. Having one available can mean the difference between landing and losing business.
- Document the control environment: A SOC 1 provides a clear explanation of the organization's control environment and the auditor's opinion of the controls.
- Improve the control environment: Both the readiness assessment and the SOC 1 examination identify weaknesses in the control environment. The auditor can also identify value-added "leading practices" used by others in their industry to meet similar objectives.
- Save the organization and customer time and money: When customers request SOC 1 reports or equivalent information, having it available saves resources. Also, SOC 1 reduces or eliminates requests and site visits from clients, prospective clients, and their auditors.
- Meet SOX requirements: SOC 1 provides public companies with documentation pertinent to SOX Section 404 and 302 attestation and related certifications.

SOC 1 helps build transparency and trust into customer relationships. Investors and customers can gain the comfort of knowing that they do business with organizations that employ proper controls and sound risk management.

Challenges Around Controls

Many control environments develop over time in piecemeal fashion. New systems and procedures are grafted onto legacy systems and procedures. New asset classes and reports may be added with limited thought to where and how they fit. New demands by customers or regulators continually arise and must be met quickly. New people are hired and veterans depart.

A number of factors may gradually and unnoticeably weaken controls including lack of documented procedures, "one-off" processing, lack of connectivity among systems, lax monitoring of third-party service providers, and insufficient segregation of duties. Add manual fixes, redundant or missing data, and complex naming conventions and transaction tracking methods and you have a control environment rife with potential gaps and shortcomings. Controls also often constitute too many extra steps or provide vital information well after the fact.

Controls generally work best when integrated into procedures and workflows. Ideally, they provide real-time identification of risks rather than after-the-fact notification. This may require a tool that sits atop a system or a dashboard that provides a window into a disbursement system. Such a tool or device can enforce compliance with procedures or flag instances of noncompliance such as transactions above thresholds or unauthorized disbursements. Yet those controls must be periodically tested and assessed for design and operational effectiveness.

An enterprise begins to build a control environment by establishing a risk management and internal control mandate and a risk management committee. That committee requires a charter that clearly designates scope, responsibilities, and risk appetite. Then an individual or function must be given responsibility for assessing risk, designing and implementing controls, and formalizing the controls through documentation and testing.

In many enterprises, these tasks are carried out by internal audit or operational risk groups or both. Indeed, internal audit generally has the skills, objectivity, and resources needed to execute these responsibilities (while appropriately leaving responsibility for managing risk to operational risk and business unit managers).

Once these tasks are complete, creating an effective control environment entails:

- Conducting a risk assessment
- Establishing and documenting control objectives
- Designing and implementing controls
- Testing and maintaining controls

Conducting a Risk Assessment

A risk assessment identifies all relevant risks the enterprise faces, details the risks within each area, and categorizes them by priority. With such an assessment, management can make informed decisions regarding risk mitigation and allocations of risk management resources. For example, areas in which to assess risks might include cash management, valuation, IT, legal, due diligence, and monitoring of third parties, to name a few.

Classification systems assign priorities to risks in light of factors specific to the enterprise and its operations. Risk assessments are developed through interviews with personnel in specific areas, reviews of data on specific transactions, knowledge of known issues, and any historical errors or breaches to policy within the organization or common to the industry. A clear understanding of each area and its complexities, interdependencies, and nuances is critical to properly assessing the risks.

Establishing and Documenting Control Objectives

Control objectives must not only be established for each risk area and risk, but also documented. In that way, the objectives can be communicated, promulgated, and used to measure the effectiveness of controls. Documented control objectives help to establish a strong control environment and assist in training new personnel.

Risk intelligent control objectives focus on regulatory compliance and risk avoidance and on risks encountered in the pursuit of value creation. Control objectives thus serve a strategic function as well as a "policing" function. When considering a new type of asset, transaction, or market, management may consider the types of controls required from the regulatory and reporting standpoints and those that will set parameters and elicit behaviors that will strike the desired balance between risk and return.

Control objectives may incorporate industry leading practices, guidelines from sources such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and specific business needs. When properly used, control objectives and controls help the enterprise to achieve efficiency and effectiveness in risk management and in operations and processes.

Designing and Implementing Controls

Controls must support the established control objectives. An obvious observation perhaps, yet in conducting assessments SVA typically locates control objectives that lack corresponding controls as well as control designs that fail to support the control objectives

To implement controls, the enterprise must develop or acquire the people, processes, and information needed to carry out control procedures. In a controls assessment, these three elements can be rated for specific qualities. For example:

- People: experience and skills of people responsible for overseeing and performing specific control activities
- Processes: presence and effectiveness of the control activities
- Information: quality of the data sources and quality and timeliness of information that support control activities

Implementation of controls calls for operational discipline which begins with enterprise leadership and extends to the employees doing the work. Yet to the extent that controls can be integrated into workflows and thus minimize the need for conscious discipline, they should be. In that way, people "manage risk" as part of their jobs rather than considering it a separate activity.

Testing and Maintaining Controls

An effective control environment always remains a work in progress. Risks by their nature are uncertain, dynamic, and driven by human behavior. They change as business conditions change, as management develops new goals and strategies, and as the enterprise adopts new methods and processes.

Therefore, controls must be periodically assessed, tested, maintained, and updated. Various internal procedures and functions, notably internal audit, can enable these important activities. Substantial guidance is available from industry groups, external auditors, and standards issued by accounting bodies.

Again, as this paper has explained, SOC 1 is an excellent example of the latter and a method of assessing, improving, and documenting controls and the control environment. While SOC 1 is intended for third parties, as are general audit opinions of financial statements, the standard provides useful guidance for management teams who aim to establish an effective control environment.

The Risk Intelligent Enterprise

In keeping with risk intelligence, SVA employs a risk-based approach tailored to the specific organization and its customers. SVA's approach to risk management enables an enterprise to:

- Address a broad spectrum of risk including compliance, security, strategic, reporting, financial, operation, IT, reputational, and other risks
- Acknowledge the need for risk specialization by function
- Consider the interaction of multiple risks and develop ways of mitigating and managing multiple threats
- Create common terms and metrics for risk and enable people to manage risk at the level of their daily activities
- Encourage risk taking for reward in addition to a risk avoidance

Risk intelligence places the SOC 1 examination in the context of the enterprise's overall approach to risk management. This in turn means that the examination will have the proper scope and level of thoroughness and the appropriate allocation of resources. SVA is also mindful of the challenges involved in establishing an effective control environment and works with management to address those challenges.

Getting Started

Undergoing a SOC 1 examination may initially seem to be a mysterious or daunting task but there are ways to ease into the process. Most commonly, an organization will begin with a readiness assessment to ascertain the requirements of SOC 1, develop the scope of the examination, and document the control objectives and descriptions. Many organizations find the SOC 1 process less overwhelming when they hire an external provider to help with this assessment. Readiness assessments vary with the needs of the organization but they can include:

- Conducting a training session on what a SOC 1 examination entails
- Considering the optimal scope of the examination and the activities to include
- Assisting with the drafting of the control objectives and descriptions
- Assessing, at a high level, controls currently in place at the organization
- Providing insights on gathering and retaining documentation and data

Whether you bring in an independent auditor to assist in a readiness assessment or do it yourself, SVA recommends that several tasks be accomplished before an initial examination:

- Determine which areas will be included in the scope, considering also whether any sub-service organizations would need to be noted in the SOC 1 report
- Draft a description of controls including relevant control objectives and the control activities that support each objective
- Determine the coverage period and date for the SOC 1 report, with typical coverage periods being 6 to 12 months
- Engage an independent certified public accountant to perform the SOC 1 examination and prepare the report
- Identify and assign internal resources to facilitate the examination and work with the accountant

A SOC 1 examination requires some effort on the part of the organization. That said, as with most such efforts, the improvements to effectiveness and efficiency, the advantage from the administrative and marketing standpoints, and the "ounce of prevention" that forestalls the "pound of cure" generally make the process thoroughly worthwhile.

Embarking On The Path To Excellence

Many organizations have found that SOC 1 provides a method and means of developing a risk management structure, establishing a proper control environment, testing and improving controls, and documenting it all in a systematic, repeatable, authoritative manner. SOC 1 guidelines provide the openness and leeway to design an infrastructure and environment that fits the organization and its customers, while providing the rigor necessary for a reliable process.

An independent auditor can assist in the readiness assessment and properly scope and conduct the examination and help the organization develop the right control objectives and the best methods of meeting them. Independent auditors' reports can help assure the organization's investors and customers of the suitability of their service organizations' processes.

Given the business and investment climate and growing demands from multiple quarters for sound risk management and controls and increased transparency, any service organization not currently employing SOC 1 can only benefit by at least considering doing so.

The information contained herein is confidential and proprietary to SVA Certified Public Accountants, SC. It is not to be disclosed, in whole or in part, without the expressed written consent of SVA Certified Public Accountants, SC. It shall not be duplicated or used, in whole or in part, for any purpose other than to evaluate the suggestions of SVA Certified Public Accountants, SC.